UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

iCloud storage accounts for xwaimzofficial@icloud.com

Case No. 16-M-1333

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A incorporated herein by reference.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B incorporated herein by reference.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ■ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 2251 and 2252A

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Christina Porter
Applicant's signature

Christina M. Porter, FBI Task Force Officer
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 12/7/16

William E. Duffin
Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT
INTRODUCTION

I, Christina M. Porter, having been first duly sworn, do hereby depose and state as follows:

1. I have been employed as a law enforcement officer with the West Allis Police Department since May of 2004, and have been a Detective with the Sensitive Crimes Unit (SCU) for approximately four years. I am currently assigned to the Child Exploitation Task Force (CETF) with the Federal Bureau of Investigation (FBI) out of the Milwaukee Field Office. While employed by the West Allis Police Department, in conjunction with the FBI, I have investigated federal and state criminal violations related to child exploitation and child pornography. I have gained experience of such investigations through formal training and in consultation with law enforcement partners in local, state, and federal law enforcement agencies. I have received training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in forms of computer media. I am a FBI Task Force law enforcement officer (TFO) who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant.

2. This affidavit is submitted in support of an application for a search warrant for information contained in, or associated with, the iCloud storage accounts of xwaimzofficial@icloud.com and thexavierwolfe@icloud.com, controlled by the web-based electronic communication service provider known as Apple Inc.

3. This affidavit is submitted under Title 18, United States Code, Sections 2703(a), 270(b)(1)(A) and 2703(c)(1)(A), and Rule 41, Federal Rules of Criminal Procedure, requiring Apple Inc., to disclose to the government records and other information in its possession pertaining

to the subscriber or customer associated with the accounts referenced in this affidavit and further described in Attachment A, including the contents of communications. Apple Inc. is located at 1 Infinite Loop, Cupertino, California 95014.

4. The facts in this affidavit are based on my personal observations, my training and experience, and information obtained from other agents, law enforcement officers and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of the facts known by me about this investigation.

5. I have probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2251and 2252A, involving the use of a computer and the Internet, is located within the aforementioned accounts. I have probable cause to believe that the member accounts that are the subject of this application will have stored information and communications that are relevant to this investigation, including evidence of the identity of the person maintaining the account and other email accounts associated with the email accounts and iCloud accounts of xwaimzofficial@icloud.com and thexavierwolfe@icloud.com. Based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in the accounts.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of Title 18, United States Code, Sections 2251 and 2252A, relating to material involving the sexual exploitation of minors. Based upon my training and experience, as well as conversations with other experienced law enforcement officers, federal prosecutors, and computer forensic examiners, I know the following:

a. 18 U.S.C. § 2251(a) in pertinent part makes it a federal crime or offense for any person to employ, use persuade, induce, entice or coerce and minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction if that person knew and had reason to know that such visual depictions would be transmitted using a means and facility of interstate commerce, that is, by computer via the internet.

b. 18 U.S.C. § 2252(A) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer.

7. The legal authority for this search warrant application is derived from Rule 41, Federal Rules of Criminal Procedure and Title 18, United States Code, Sections 2701 et seq., titled "Stored Wire and Electronic Communications and Transactional Records Access."

8. Title 18, United States Code, Section 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703(a) & (b), as amended by the USA PATRIOT Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation.

DEFINITIONS

9. The following definitions apply to this Affidavit and attachments hereto:

1. I have viewed the Apple Inc. Legal Process Guidelines, dated September 2015, and I know from reading that document that Apple Inc. keeps data uploaded into an iCloud account by an individual user of the iCloud service. The iCloud account is linked to the user by his Apple ID, and the contents stored in the account are determined by the user. The contents could be any or all of the following:

- Subscriber and billing information
- Mail logs
- Email content
- Photo stream
- Documents
- Contacts
- Calendars
- Bookmarks
- IOS device backups, including photos and videos in the users' camera roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail

10. "Cloud storage" is an online central storage location, which allows users to access their files from anywhere using a device connected to the Internet. "iCloud" is a cloud storage and cloud computing service from Apple Inc. The service allows users to store data on remote computer servers for download to multiple devices, to include smart phones and computers.

11. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, Apple Inc., and Google, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet.

INFORMATION REGARDING APPLE INC. EMAIL AND ICLOUD ACCOUNTS

12. Through my training and experience, as well as review of materials provided to me by Apple Inc. and other experienced law enforcement officers, I have learned that Apple Inc. provides a variety of online services, including electronic mail ("email") access, to the general public. Apple Inc. allows subscribers to obtain email accounts at the domain name "iCloud.com" like the email account listed in Attachment A. Subscribers obtain an account by registering online with Apple Inc. During the registration process, Apple Inc. requires subscribers to provide basic personal information. Therefore, the corporate servers of Apple Inc. are likely to contain stored electronic communications (including retrieved and un-retrieved email for iCloud subscribers) and information concerning subscribers and their use of Apple Inc. and iCloud services, such as account access information, email transaction information, and account application information.

13. I have learned that an email that is sent to an Apple Inc. iCloud subscriber, is stored in the subscriber's "Inbox" on Apple Inc. servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Apple Inc. servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, Apple Inc. and other cloud storage services, such as Google Drive, Dropbox, and SkyDrive, have provided their users with larger storage capabilities associated with the user's account. Apple Inc. starts users out with 5 gigabytes of storage space, and if the user begins to fill that space up, the user can pay for additional storage space. Based on my training and experience, and conversations with other law enforcement officers with experience in executing search warrants of email accounts, I know that search warrants for email accounts and computer media may reveal stored emails sent and/or received long prior to the date of the search.

14. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that when the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Apple Inc.'s servers, and then transmitted to its end destination. Apple Inc. often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Apple Inc. servers, the email can remain on the system indefinitely.

15. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that a sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by Apple Inc., but may not include all of these categories of data.

16. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that an iCloud subscriber can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, videos and other files on servers maintained and/or owned by Apple Inc. Subscribers to an iCloud account might not store on their home computers copies of the emails stored in the iCloud account. This is particularly true when they access their iCloud account through the web, or if they do not wish to maintain particular emails or files in their residence. In essence, a subscriber's email box has become a common online data storage location for many users.

17. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that in general, email providers like Apple

Inc. require each of their subscribers provide certain personal identifying information when registering for an email account. This information could include the subscriber's full name, physical address, telephone numbers and other identifiers, such as alternative email addresses, and, for paying subscribers, means and source of payment (including a credit card or bank account number).

18. Based on my training and experience, I know that email providers typically retain certain transaction information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account associated with Apple Inc.'s website(s)), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account, as well as the geographic location of these devices.

19. Based on my training and experience, I know that in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the providers support services, as well as records of any actions taken by the provider or user as a result of the communications.

20. Based on my training and experience, I know individuals often use email accounts for everyday transactions because it is fast, low-cost, and simple to use. People use email to communicate with friends and family, manage accounts, pay bills, and conduct other online business. Email users often keep records of these transactions in their email accounts, to include identifying information such as name and address.

21. Based on my training and experience, I know that evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and other files.

22. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that an Apple ID is an all-in-one email address that is used to log into various online systems that Apple Inc. offers for many of its products. Users of Apple Inc. products such as "iTunes" and "Photostream" can have one Apple ID that corresponds to their accounts, and one of the services available through Apple Inc. is iCloud storage. Apple Inc. offers the ability to link all of its products through an iCloud account.

23. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that iCloud is a file hosting, storage, and sharing service that is provided for iCloud account users. iCloud has been integrated into Apple Inc. and is linked to, associated with, and accessible using an iCloud email account. The integration allows users to directly upload documents and photos within the iCloud account, store them on iCloud, and share with other users.

24. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that an Apple Inc. iCloud account allows

users to upload files, photos, and favorites on Apple Inc. servers to cloud storage, and allows members to access them from any computer with an Internet connection. After uploading photos and/or files to iCloud, one can share the photos and other files with friends or to anyone on the iCloud network. The user can send an email, using the user's iCloud email account, to other individuals inviting them to view the photos and files. The service allows the user to keep the files private, share only with specific contacts, or make the files public. Publicly shared files do not require an Apple Inc. iCloud account to access; the service offers five (5) gigabytes of free personal storage.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

25. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals who collect child pornography. I have observed and/or learned about the reliability of these commonalities and conclusions involving individuals, who collect, produce and trade images of child pornography. Based upon my training and experience, and conversations with other experienced agents in the area of investigating cases involving sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography collect sexually explicit

materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, Peer-to-Peer (P2P), email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other likeminded individuals over the Internet. As such, they tend to maintain or "hoard" their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. Based on my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who possess, receive, and/or distribute child pornography by computer

using the Internet often maintain and/or possess the items listed in Attachment B.

26. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with law enforcement officials.

27. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage to their collection of illicit materials. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures or send it to third party image storage sites via the Internet.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

28. On June 14, 2016, I was assigned to follow-up on a lead from the FBI-Chicago office, from TFO Jacqueline Lazzara that stems from a child pornography investigation she had conducted.

29. TFO Lazzara, while investigating a separate incident, conducted an interview with Daniel Santiago (hereinafter "Santiago") in Illinois. During the interview, Santiago stated that he was communicating with two boys online, whom he believed to be minors, named CH (full name is known to law enforcement) and Xavier Douglas. Santiago said he had sent gifts totaling $12,000 to CH and approximately $400 and an X-Box to Xavier Douglas. Santiago sent gift cards to CH through CH's email account of C[redacted]h[redacted]@gmail.com. Santiago said Xavier's email address is

xavier@gmail.com. He communicated with CH and Xavier Douglas on Twitter and KIK Messenger.

30. Santiago stated during the interview he thought CH resided in Pennsylvania and Xavier Douglas lived in Waukesha, Wisconsin. TFO Lazzara determined that a juvenile boy named CH did reside in Pennsylvania and a lead was sent to agents in Pennsylvania to locate and interview CH. CH's parents were interviewed and a forensic interview was conducted with CH. CH is currently 16 years old.

31. During the forensic interview, CH stated he did not recognize Daniel Santiago's name, usernames, or photos. CH stated that in the fall of 2014 he met an individual on KIK (a free instant messenger application for mobile devices which is known for its features preserving users' anonymity) who he thought was a female juvenile of his own age. The individual used the screen name of "littlelainey12" while communicating with CH via KIK.

32. CH stated in his interview that "littlelainey12" sent him pictures of herself, which he believed were not real, and CH sent "littlelainey12" photos of himself, including nude photos. Over time, "littlelainey12" threatened CH that if he didn't send more photos, "littlelainey12" would put CH's nude photos on the Internet. CH sent additional photos of himself to "littlelainey12" using a dropbox account provided by "littlelainey12." At times CH would send 250 photos to "littlelainey12."

33. CH reported that he observed his photos on the Internet, specifically on Twitter. CH's mother, SH (full name known by law enforcement), also saw websites with CH's photos and reported it. The National Center for Missing and Exploited Children (NCMEC) has a report regarding a Twitter account called "ClayExposed" that comes back to thexavier@ail.com. The

account contains child pornography.

34. TFO Lazzara advised that based on her investigation, it appears the individual behind the account "littlelainey12" forced CH to take photos of himself and used his identity to talk to Daniel Santiago. TFO Lazzara served a subpoena for information concerning claybaby34@gmail.com, one of the email addresses CH provided during his forensic interview, as an email address being associated with him, but were unfamiliar to CH. The information provided revealed claybab34@gmail.com is registered to a recovery email of xdouglas177@gmail.com and to an IP address of 65.30.129.50. TFO Lazzara also served a subpoena for c[redacted]h[redacted]@gmail.com, which was provided by CH during his forensic interview, and it is registered to the same IP address of 65.30.129.50. CH advised he has never created a gmail account for himself.

35. The IP address of 65.30.129.50 comes back to Time Warner Cable. TFO Lazzara sent a subpoena to Time Warner Cable for this IP address and the IP address is registered to Marcy Wolfe of XX32 Northview Road, Waukesha, WI and has been an active account since February 1, 2009. When TFO Lazzara tried to find out who Xavier Douglas could be, she found a police report from Jefferson County (#2014CF000018) for criminal trespass. Xavier Douglas is currently on probation for this offense.

36. The NCMEC Cybertip reported that the same IP address of 65.30.129.50 was used to create the "ClayExposed" Twitter account on December 1, 2015 at 04:40UTC, which contains child pornographic images of CH.

37. I reviewed the images provided in the NCMEC tip, which were from the Twitter URL of https://twitter.com/ClayExposed/status/671550766419566593. The incident date and time are December 1, 2015 at 04:45:24UTC. One image I viewed was file CVHT25sUEAQnJbh.jpg,

which is an image of a white male who appears to be taking a "selfie" picture. He is nude and is holding his penis with his right hand. A portion of the male's face can be seen and he appears to be approximately 12-15 years old. The male appears to be in the beginning stages of puberty as he has some pubic hair, but there is a lack of hair on his face and chest. A second image I viewed was file CVHTv1wUsAANMOg.jpg, which is an image of the same white male taking a "selfie" picture in a mirror with a gold colored frame. The male is holding a cell phone in his left hand and pulling up his gray long-sleeved shirt with his right hand, exposing his penis. His black pants are pulled down around his thighs. His face is exposed and he is wearing a gray winter hat.

38. I spoke with TFO Lazzara who advised that images of CH were posted online with his soccer team in Pennsylvania. I conducted a Google Internet search of CH and located images of CH with his soccer team. I observed that these images are of the same male from the child pornographic images in the ClayExposed Twitter account.

39. On June 15, 2016, I reviewed all of the supplemental information provided with the lead from TFO Lazzara. It is her belief, based on her investigation, that whoever is using the IP address of 65.30.129.50 is "littlelainey12" and had CH take child pornographic pictures of himself and then used CH's identity and photos to talk to Daniel Santiago, and coerced Santiago to send gifts valued at $12,000. I ran an NCIC/DOT check and an Accurint check on Xavier Douglas. I located two possibly addresses for Xavier in Waukesha, WI, one being XX32 Northview Road.

40. On June 15, 2016, I made contact with Xaiver's probation agent, Tracy Kaczek. Agent Kaczek advised that she conducts home visits at Xavier's residence and he is currently residing at XX32 Northview Road in Waukesha. He resides with his sister and her family. Xavier's sister is Marcy Wolfe, which is where the IP address in question lists to. There is a toddler between the

age of one and two who resides at the residence with whom Xavier has regular contact. Agent Kaczek advised that she would be entering a warrant into NCIC for Xavier's arrest.

41. I made contact with Detective Edward Bergin of the Waukesha Police Department. Detective Bergin advised that his department had contact with Xavier Douglas on March 16, 2016, regarding a down power line. Xavier reported his address to be XX32 Northview Road at that time.

42. On June 20, 2016, FBI Agent Mustell and I went to XX32 Northview Road and conducted a check of the open WIFI signals outside the residence. Of the various signals in the area, two signals are labeled as Wolfe and Wolfe Guest. Both of these signals, as well as all other signals in the area, were secure.

43. On June 20, 2016, I checked Facebook for any accounts listing to Xavier Douglas. I located a profile named "Xavier Douglas (Real Xavier)" with the URL of https://www.facebook.com/xavier.douglas.963. The image on the profile picture matched Xavier's Department of Transportation photo, so I believed this is his account. I observed a message posted on this Facebook account from August 27, 2013 which stated, "OK So I like younger white guys. Can you blame me? And when they don't feel the same way about me, I steal their pics and create fake profiles and pretend they are my friends and tweet about it all day and all night. My name is Xavier and I am the best Waukesha has EVER produced." This post was followed by a photo of a young, white male's face who appeared to be around eight years old. I sent a preservation request to Facebook to maintain this profile.

44. I obtained a search warrant and executed it on June 30, 2016 at Xavier Douglas' Waukesha residence. Xavier was taken into custody based on his DOC warrant. Xavier agreed to speak with

FBI Agent Banner and myself at the Waukesha County Sheriff's Department. During the interview, Xaiver admitted that he took over other peoples' identities to create social media accounts. He stated he wanted to become famous, or more popular, on social media because once a person obtained a certain amount of attention on various social media sites, the site compensates you for using their service.

45. Xavier explained during the interview that over the last three or so years he sought out social media accounts utilized by attractive male teenagers who were already popular online and who had a significant number of friends and online attention. Xavier named four boys who were popular online as Gage Smith, Gage Parris, Andrew Lauro, and Garrett Bosely. Xavier said he created fake social media accounts using these names and operated these accounts. Several people began to befriend and follow these individuals, not knowing that Xavier was posing as these boys. As these accounts grew in popularity, Xavier posed as the boy named on the account and posted information about Xavier's real, personal social media accounts. He promoted his own accounts and more people would befriend him so he would gain popularity.

46. During the interview, Xavier was asked about CH and Xavier admitted that he located CH on Instagram and found CH's KIK or Snap Chat username listed on the Instagram account. Xavier admitted to creating the "littlelainey12" username and account to communicate with CH via KIK or Snap Chat. Xavier admitted to obtaining nude images of CH because he is attractive and Xavier wanted to "leak" the images online for more attention. After Xavier obtained initial images from CH, Xavier admitted that he told CH he would expose the images CH had already provided online if CH didn't take additional child pornographic images. CH then provided Xavier with additional images via Dropbox.

47. During the interview, Xavier also admitted to creating social media accounts in CH's name and operated those accounts. After gaining numerous friends/followers, he posted a message in CH's name which stated that some of his pictures had been leaked. Xavier admitted to creating a Twitter account labeled "ClayExposed" or "ClayH---Exposed" which included the nude images that he obtained from CH.

48. During the interview, Xavier was asked about Santiago. He said Santiago had contacted CH via one of the social media accounts that Xavier was operating in CH's name. Xavier said that Santiago wanted friends and offered to send Xavier gifts in return for a continued online friendship. Xavier admitted that Santiago sent him a laptop and an X-Box gaming console. Santiago thought he was sending the items to CH, but he told Santiago that CH was worried about giving out his address, so instead he was going to provide a friend's address. Xavier, then posed as CH, provided Santiago with the name of Xavier Douglas and Xavier's address.

49. Xavier provided consent for agents to take over his Dropbox account. On July 18, 2016, I examined the contents of the account. Under the "Camera Uploads" section of the account, there are 193 pictures/videos. I observed an image of a nude, erect penis, in addition to selfie-style pictures of CH in a mirror, CH with other teenagers, and CH at school.

50. During the search of Xavier's residence, a black iPhone with serial number 579CE2816A was located. It was identified as belonging to Elizabeth Wolfe, who is Marcy Wolfe's juvenile daughter who also resides with Xavier. Both Elizabeth and Xavier admitted that the phone belonged to and was used by Xavier before it was given to Elizabeth. The cell phone was collected as evidence and was forensically examined at the FBI.

51. I reviewed the cellphone extraction report. I located references to CH in the Chats section

of the phone report, contacts section, calendar section, and images section. I also located a picture of a male holding a phone for a Facebook profile picture and the image is labeled "Gage Parris." I observed an image of CH in a sports uniform, in addition to other pictures of CH. In the "contacts" section of the report, I located the name "Xavier" followed by the contact of xwaimzofficial@icloud.com, which is believed to be Xaiver's email address associated with one of his iCloud accounts.

52. Also collected during the search warrant was an Apple iPad MD510 which was later analyzed. Per the extraction report, a contact listed in the iPad was thexavierwolfe@icloud.com, which is believed to be another email address associated with one of Xavier's iCloud accounts.

53. During the search warrant, Xavier's Acer laptop computer (product ID of 00325-91035-19011-AAOEM) was collected as evidence. He admitted to being the only user of the laptop. The laptop was forensically analyzed. On July 26, 2016 I reviewed the contents report. Under the Google search section, some of the terms searched included twitter, you tube, facebook, iphone 5 se clone, unfollow everyone on Twitter, delete all my tweets, how to view photos on my icloud, lock my iphone, icloud, and download photos from icloud to pc. Based on these searches, I believe Xavier was utilizing iCloud storage.

54. Based on my training, experience and conversations with other trained and experienced investigators, I know that suspects as well as private citizens are heavily using "cloud" services. Cloud services allow the user to store their data on remote servers which they do not have physical access to. A user can access this remotely stored data from all types of digital devices with access to the internet including mobile devices such as cellular phones, tablets and laptops as well as from traditional desktop computers. Cloud service provider also may store location data which can be

used to determine where the user's device(s) were located at a given date and time. The user typically owns and controls the data stored on the remote server(s) while the electronic service provider owns the server on which data is stored.

55. I know that many digital devices utilize the "cloud" services to store backups and/or data which can be accessed from multiple sources. I know that many digital devices are using cloud services by default, sometimes without the user's knowledge. This use of cloud storage has become so closely tied with many devices that the cloud functions as an extension of their digital device; for this reason, persons may have data on the cloud that is not present on the digital device. Common cloud services are Facebook, KIK, SnapChat, Dropbox, Google Drive, iCloud, and web-based email services such as Gmail and Yahoo to name just a few.

56. It is also my training and experience that cellular telephones are now being utilized by suspects, as well as private citizens, for the purposes of portable computing using cloud services. Many cellular telephones have the ability to; type and store documents, take and store pictures/videos, access the Internet, deploy applications, make phone calls, send and receive SMS/MMS messages and chats, connect to social networks, remotely store data on the "cloud", store large amounts of data on the actual phone, sync with a computer, and show live video streaming.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

57. I anticipate executing this warrant pursuant to the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Apple Inc. to disclose to the government copies of the records and other information (including the content of communications) more particularly described in

Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

58. Based on my training and experience, and the facts as set forth above, I have probable cause to believe that on the computer systems in control of Apple Inc., there exists evidence of a crime(s), contraband and/or fruits of a crime(s). Specifically, I have probable cause to believe that the email accounts and iCloud storage accounts of xwaimzofficial@icloud.com and thexavierwolfe@icloud.com, described in Attachment A, will contain evidence, fruits, and instrumentalities of a crime(s), that is violations of Title 18, United States Code, Sections 2251, 2252, and 2252A. Accordingly, a search warrant is requested.

59. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711(3), and Title 18, United States Code, Sections 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." Title 18, United States Code, Section 2711(3)(A)(i).

60. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

This warrant applies to information contained in and associated with the Apple Inc., email accounts and iCloud storage accounts of "xwaimzofficial@icloud.com and thexavierwolfe@icloud.com" which are stored at the premises owned, maintained, controlled, and operated by Apple Inc., 1 Infinite Loop, Cupertino, California 95014.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

I. **Information to be disclosed by Apple Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple Inc., Apple Inc. is required to disclose the following information to the government for the account(s) listed in Attachment A. Such information should include the following:

1. The contents of all emails, instant messages and/or other communications stored in the email accounts for "xwaimzofficial@icloud.com and thexavierwolfe@icloud.com," for the period from July 1, 2014 through the current date, including copies of emails and instant messages sent to and from the account, draft emails and instant messages, the source and destination addresses associated with each email and/or instant message, the date and time at which each email/instant message was sent, and the size and length of each email/instant message;

2. Any and all deleted emails, instant messages and/or other communications that are still maintained and/or preserved by Apple Inc., including any information described in paragraph 1 above for the period from July 1, 2014 through the current date;

3. Any and all photographs, videos, visual depictions, instant messages or other content stored in the iCloud accounts for "xwaimzofficial@icloud.com and thexavierwolfe@icloud.com," and all information pertaining to the source of such photographs, videos, visual depictions, messages, and other stored content for the period from July 1, 2014 to the current date, including any and all photographs, videos, visual depictions, instant messages or

other content that the user may have deleted or attempted to delete but that are still maintained and/or preserved by Apple Inc.;

4. All records or other information regarding the identification of the accounts for the period from July 1, 2014 to the current date, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

5. All records or other information stored by any individual using the account, including profile, address books, contact and buddy lists, calendar data, pictures, and files for the period from July 1, 2014 to the current date;

6. All records pertaining to communications between Apple Inc., and any person regarding the accounts, including contacts with support services and records of actions taken for the period from July 1, 2014 to the current date.

7. All records associated with other services provided with an iCloud account, to include: iCloud, Groups, Office, Photos, Spaces, iTunes and iPhone for the period from July 1, 2014 to the current date.

II. **Information to be seized by the government**

All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code,

Sections 2251, 2252, and 2252A, and also including, for the accounts listed on Attachment A, the following items:

1. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the accounts listed on Attachment A;

2. Evidence of who used, owned, or controlled the accounts listed on Attachment A;

3. Evidence of the times that the accounts listed on Attachment A was used;

4. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.